DATA PRIVACY RIGHTS IN THE UNITED STATES

by
Cristy Villalobos Hauser

A capstone project submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Public Management

Baltimore, Maryland
December 2021

Abstract:

As American consumers download and use software applications, their data is collected by corporations. The personal data of Americans is lucrative in today's digital market. The consent of consumers is not necessary for their personal information to be sold or shared with a third-party entity. However, in other countries like the European Union (EU), it is illegal to share personal data of consumers without their consent. The EU has comprehensive data protection law to secure the data privacy rights of its residents. In the United States, there is no comprehensive federal protection law to secure the personal data of consumers. This memo highlights the history of data privacy rights, a policy proposal, a political proposal, and a final recommendation to secure the data privacy of Americans. This capstone further evaluates a data protection legislation proposal, S.2134 bill, drafted by United States Senator Kirsten Gillibrand, in 2021.

Advised by: Professor Paul Weinstein Jr.

Acknowledgments

To my family, Theodore Hauser, Kylo Hauser, Ernestina, and Lazaro Villalobos, who have encouraged me through this program. I am eternally grateful for the support of my brothers and sisters-in-law as well. Thank you for all of your support.

To my advisor, Paul Weinstein, thank you for counseling me through this Capstone writing process.

Table of Contents

List of Figures

Date: September 2, 2021

To: Congresswoman Jennifer Wexton

From: Cristy Villalobos Hauser

Subject: Data Privacy Rights in the United States

Action Forcing Event: This week, the European Union (EU) authorities fined Facebook's WhatsApp messaging application $266 million for violating the General Data Protection Regulation (GDPR).[1] The EU'S GPPR is a data protection legislation that requires technology companies to disclose how the data was shared with its other companies.[1] WhatsApp breached the GDPR by sharing data with other Facebook companies such as Instagram.[2] Big technology companies like Google and Amazon have also violated the data rights of consumers in the E.U., meanwhile online consumers in the U.S. don't have online privacy rights under Federal law.

[1] Mohan, B. (2021, September 2). *WhatsApp hit with a $266 million fine for violating EU data privacy laws*. Android Central. https://www.androidcentral.com/whatsapp-hit-266-million-fine-violating-eu-data-privacy-laws.

[2] Satariano, A. (2021, September 2). *Facebook's WhatsApp is fined for breaking THE e.u.'s data privacy law.* The New York Times. https://www.nytimes.com/2021/09/02/business/facebook-whatsapp-privacy-fine.html

Statement of the Problem: Lack of Data Privacy Rights in the United States

Under the original Constitution, Americans were not explicitly granted a right to privacy. The right to privacy was interpreted by the Supreme Court. The Fourth Amendment has explicitly protected Americans from unreasonable search and seizure without a warrant. The Supreme Court ruled that the Fourth Amendment provided "the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[3] The Fourth Amendment protects people against unreasonable government searches. Over time, the Fourth Amendment helped to develop a right to privacy in the common law.

Former Supreme Court Justice Louis Brandeis defined privacy as "the right to be let alone" in 1890.[2] Brandeis later developed privacy torts laws to protect the privacy rights of individuals from "unreasonable intrusion upon the seclusion of another, appropriation of other's name or likeness, unreasonable publicity given to other's private life, and publicity that unreasonably places the other in a false light before the public." [4] His work developed the right to privacy in contemporary American law. The Supreme Court established a constitutional right to privacy in *Griswold v. Connecticut* in 1965 with Brandeis's definition of privacy. The Due Process Clauses of the Fifth and Fourteenth Amendments also lead to the creation of privacy as a right.[5]

Then, the concept of data privacy originated in the late 20th century with the introduction of the internet and its accessibility on computers and cellular devices. Data privacy refers to the specific kind of privacy linked to personal information that is provided to private actors in a variety of different contexts. For example, an online user's personal information could be collected by a software application, which then safeguards that personal information.

[3] "Protecting Privacy under the Fourth Amendment." The Yale Law Journal. Yale University, 1981. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=6716&context=ylj.
[4] Ben Bratman, "Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy," Tennessee Law Review 69, no. 3 (Spring 2002): 623-652
[5] Hart, C. (2021, August 12). *A beginner's Guide to Data Privacy*. Northeastern University Graduate Programs. Retrieved November 16, 2021, from https://www.northeastern.edu/graduate/blog/what-is-data-privacy/.

Further, the Congress Research Service (2019) defined data protection "as a legislative concept, data protection melds the fields of data privacy (i.e., how to control the collection, use, and dissemination of personal information) and data security (i.e., how to (1) protect personal information from unauthorized access or use and (2) respond to such unauthorized access and use. (1). (p.1)" [6] Federal laws have addressed these issues separately, however, there is a trend to combine both of these definitions along with a unified legislative bill.[6] Since the federal government does not have a comprehensive data protection law, businesses must abide by sector-specific laws.

Consequently, the United States federal government does not restrict the transfer of personal data to other jurisdictions. Businesses are given the authority to transfer the personal information of users in compliance with applicable transfer rules such as consent of data subject, a contract with the consumer, compliance with a legal obligation. Currently, it is not a requirement for online users to be notified when their data is shared from one business to a third-party entity. In the United States, there is no formal guidance on data protection. However, the Federal Trade Commission provided that a company's data security measures for data protection must be "reasonable" when considering the volume, sensitivity of data, size, complexity, and tools to address cyber vulnerabilities. [7] Companies may receive penalties for data security breaches by the Federal Trade Commission for failing to properly secure the personal information of individuals.

As a result, half of Americans believe that their data is less secure now than it was five years ago, according to the Pew Research Center.[8] The public opinion of online users has been impacted by massive data breaches in the private sector, inefficient data security practices, and the selling of personal data. Recent cyberattacks have resulted due to inefficient data security practices in the private sector, millions of Americans have had their personal information compromised. The largest data breaches of American companies consist of:

[6] Congressional Research Service. Mulligan, S. P., & b, C. D. (2020). *Data protection and privacy law: an introduction.* Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11207/2

[7] Group, G. L. (2021, June 7). *Data Protection 2021: Laws and Regulations: USA: ICLG*. International Comparative Legal Guides International Business Reports. Retrieved November 17, 2021, from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

- Yahoo's 2013 beach was announced in 2016. Over three billion user accounts were exposed. Hackers accessed account information such as security answers, passwords. [9]
- Linkedin's 2021 breach impacted 700 million users. Over 90% of its user base was posted on a dark web forum in June 2021.[10]
- Facebook's 2019 breach impacted over 533 million users. Their phone numbers, account names, and Facebook IDs were posted on the internet and the dark web.[10]
- Marriott International's 2018 breach impacted over 500 million customers. An unauthorized entity copied and encrypted information from the guest database. The data seized included names, mailing addresses, phone numbers, email addresses, passport information, date of birth, gender, and payment card information.[11]

Interestingly, the number of data breaches in 2021 has exceeded the total in 2020. According to Info Security Group, there have been 1,111 data breaches from cyberattacks this year.[12] This figure consists of traditional breaches with a third party who stole data from organizations and cloud misconfigurations that lead to information leaks to the public. There has been an increase of 27% in 2021 compared to the previous years.[12] In total, 160 million online users have had their data compromised this year due to insufficient security systems in the private sector.[13] For example, a major cybersecurity attack that has occurred in 2021 was the Colonial Pipeline cyberattack. The Colonial Pipeline company paid 4.4 million in bitcoin to the hackers. However, the Federal Bureau of Investigation was able to retrieve the ransom payment but was unable to identify the entities behind the attack.[14]

---

[8] Council on Foreign Relations. (2018, January 30). *Reforming the U.S. approach to data protection and privacy*. Council on Foreign Relations. Retrieved November 17, 2021, from https://www.cfr.org/report/reforming-us-approach-data-protection.

[9] Selyukh, Alina. "Every Yahoo Account That Existed in Mid-2013 Was Likely Hacked." NPR. NPR, October 3, 2017. https://www.npr.org/sections/thetwo-way/2017/10/03/555016024/every-yahoo-account-that-existed-in-mid-2013-was-likely-hacked.

[10] Swinhoe, Dan, and Michael Hill. "The 15 Biggest Data Breaches of the 21st Century." CSO Online. CSO, July 16, 2021. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[11] Perlroth, Nicole, Amie Tsang, and Adam Satariano. "Marriott Hacking Exposes Data of up to 500 Million Guests." The New York Times. The New York Times, November 30, 2018. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

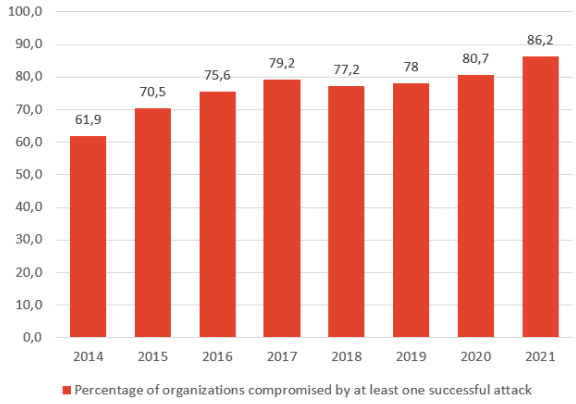
[12] Phil Muncaster UK / EMEA News Reporter. (2021, October 7). *Breach volumes for 2021 already exceed 2020 total*. Infosecurity Magazine. Retrieved November 18, 2021, from https://www.infosecurity-magazine.com/news/breach-volumes-2021-exceed-2020/.

[13] Lohrmann, D. (2021, October 10). *Data breach numbers, costs, and impacts all rise in 2021*. GovTech. Retrieved November 19, 2021, from https://www.govtech.com/blogs/lohrmann-on-cybersecurity/data-breach-numbers-costs-and-impacts-all-rise-in-2021. [8] Lovejoy, Ben. "US GDPR-Style Federal Privacy Law 'Should Replace Mess of Separate Laws'." 9to5Mac. 9to5Mac, September 8, 2021. https://9to5mac.com/2021/09/08/us-gdpr-style-federal-law/.

[14] Romo, V. (2021, June 7). *U.S. has recovered some of the millions paid in ransom to Colonial Pipeline Hackers*. NPR. Retrieved November 20, 2021, from https://www.npr.org/2021/06/07/1004050873/u-s-retrieves-some-of-the-colonial-pipeline-ransom.

Recently, there has been an increase in cyberattacks since the pandemic began in 2020. The graph below indicates that cyberattacks are on the rise more and more every year. [15] Most companies are not prepared to handle cybersecurity attacks, according to Retarus Corporate Blog. 80% of IT employees and security leaders believe their companies lack sufficient protection against cyber-attacks despite increased security expenses in 2020. Overall, this indicates that businesses are vulnerable to being compromised now more than ever before.

Figure 1. Cyberedge Group 2021 Cyberthreat Defense Report



Source: Cyberedge Group 2021 Cyberthreat Defense Report – a comprehensive review of 1,200 IT security professionals representing 17 countries and 19 industries

Moreover, the United States federal government has enacted industry-specific data protection rules for financial institutions, health care institutions, and communications carriers. However, the United States federal government does not have a comprehensive federal law that encompasses the privacy of all types of data. The data collected by companies on the daily basis is not regulated. Due to a lack of federal regulations, companies are not required to abide by specified security standards. As a result, in most states, companies can share, use, or sell any data personal data to third-party data brokers without notifying consumers.

[15] *15 biggest cybersecurity attacks in 2021*. Privacy Affairs. (2021, October 18). Retrieved November 18, 2021, from https://www.privacyaffairs.com/cybersecurity-attacks-in-2021/.
Stainer, P., & *, N. (2021, November 18). *Alarming cybersecurity statistics for 2021 and the future.* Retarus Corporate Blog - EN. Retrieved November 18, 2021, from https://www.retarus.com/blog/en/alarming-cybersecurity-statistics-for-2021-and-the-future/.

Then, third parties can sell and share the data with others without notifying consumers. [16] Data privacy rights are more safeguarded in Europe than in the United States.

As a result of companies mishandling personal data, Europe passed a General Data Protection Regulation (GDPR) in 2018 to mandate companies to ask for permission to share data and acknowledge individuals' rights to access, delete, and control the use of their data. The GDPR sets a new standard for consumer data rights and security standards. The GDPR protects basic information, IP addresses, cookie data, RFID tags, health data, biometric data, racial data, political data, and sexual orientation data. Europe has fined Facebook 267 million due to data-sharing in violation of the GDPR.[17]

While the data privacy rights of consumers are protected in the European Union, the data privacy rights of most American consumers are not protected under the federal government. Even though technology companies are fined overseas for sharing personal data without the consumer's consent, consumers do not have those same protections in the United States. The federal government has a history of providing consumers with sector-specific data rights with limited enforcement. The United States may establish the data rights of consumers now that the digital space has become more popular during the pandemic, however legislative proposals have yet to be passed through both House and Senate chambers.

[16] Lovejoy, Ben. "US GDPR-Style Federal Privacy Law 'Should Replace Mess of Separate Laws'." 9to5Mac. 9to5Mac, September 8, 2021. https://9to5mac.com/2021/09/08/us-gdpr-style-federal-law/.

[17] Nadeau, Michael. "What Is the GDPR, Its Requirements, and Facts?" CSO Online. CSO, June 12, 2020. https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.

Background/History:

Since the beginning of the digital age, the federal government has passed legislation to address emerging data protection issues. Historically, Congress enacted several federal laws to protect the data privacy of individuals in specific sectors. Since the Supreme Court ruled that the Constitution provides individuals with a right to privacy, it is only guarded against government intrusion. In response to this limitation, Congress passed federal laws to provide statutory protections of individuals' data. [18] The federal laws aren't comprehensive and uniform, but they address certain industries and subcategories of information. The set of data privacy laws include:

- Children's Online Protection Act provides data security requirements for information collection regarding children by online operators.
- Communications Act of 1934 includes data security requirements for common carriers, cable operators, and satellite carriers.
- Computer Fraud and Abuse Act prohibits the unauthorized access of protected computers.
- Consumer Financial Protection regulates deceptive, unfair, and abusive acts in connection with consumer financial services and products.
- Electronic Communications Privacy Act bans the unauthorized access or interception of electronic communications in storage or transit.
- Fair Credit Reporting Act protects the collection and use of data included in consumer reports.
- Federal Securities Laws require data security controls and data breach reporting responsibilities.
- Federal Trade Commission Act (FTC) prohibits unfair or deceptive acts or practices (UDAP).
- Gramm-Leach Bliley Act regulates financial institutions' use of nonpublic personal information.

[18] Mulligan, Stephen, and Chris Linebaugh. "Data Protection and Privacy Law: An Introduction - Congress." Data Protection and Privacy Law: An Introduction. Congressional Research Service, May 9, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11207.

- Health Insurance Portability and Accountability Act (HIPAA) regulates health care providers' collection and disclosure of protected health information.
- Video Privacy Protection provides privacy protections related to video rental and streaming.

Consequently, the Federal Trade Commission Act's ban on "unfair or deceptive trade practices"(UDAP) has been applied to the enforcement of data protection of these laws.[19] The Federal Trade Commission (FTC) brought hundreds of enforcement actions based on data violation allegations against companies. The FTC punishes companies that perform deceptive practices with the personal data of consumers in a manner that contradicts their privacy policy and companies that fail to protect personal data from unauthorized access. Companies are held accountable for their data privacy and security promises. Also, the FTC has suggested that it is unfair when companies have default privacy settings that are hard to change or when companies re-write their privacy policy retroactively.

While the Federal Trade Commission's UDAP ban provides some legislative protection to consumers, the Commission's authority is limited. The FTC doesn't mandate companies to sector-specific data protection laws. The FTC does not require companies to comply with the specific data protection policies and does not reach entities that have not made explicit promises about data protection. Overall, the FTC has limited authority over the regulation of data protection and data privacy.

As a result, three states in the United States have passed their data privacy protection laws. Currently, California, Virginia, and Colorado have comprehensive consumer privacy laws in place. The rules apply to companies that collect data from consumers in these three states. These states have similar provisions that give consumers notice and choice in data collection. Companies are required to notify consumers once their data is sold. Consumers have a chance to agree with the selling of their data. They also have the right to access, delete, correct, and move their data. [20]

[19] "The Federal Trade Commission's Regulation of Data Security ..." The FTC's Regulation of Data Security Under Its UDAP Authority. Congressional Research Service . Accessed October 1, 2021. https://sgp.fas.org/crs/misc/R43723.pdf.

[20] Hutnik, Alysa Z., Aaron J. Burstein, and Lauren F. Myers. "Colorado Passes Privacy Bill: How Does It Stack up against California and Virginia?" Ad Law Access, July 9, 2021. https://www.adlawaccess.com/2021/06/articles/colorado-passes-privacy-bill-how-does-it-stack-up-against-california-and-virginia/.

Additionally, California's privacy protection law is the strongest in the US, according to experts. California Consumer Protection Act (CCPA) allows consumers to sue companies against certain data breaches. This law allows consumers to claim damage over data privacy violations. California granted consumers the “right to know” information that businesses have collected or sold regarding them. This requires businesses to inform consumers about the personal data collected. [21] Additionally, consumers are given the "right to opt-out of" the sale of their personal information. Under the CCPA, businesses are required to inform consumers of this right and if a consumer opts out, the business is prohibited from selling the consumer’s data. Thirdly, the CCPA grants consumers the right to request that a business delete any information collected about them. This is referred to as the “right to delete”. [21]

Then several bills were recently drafted regarding data protection. Senator Kirsten Gillibrand (D-NY) proposed the Data Protection Act. Sen Sherrod Brown proposed the Data Accountability and Transparency Act. Senator Maria Cantwell’s (D-Wash.) Consumer Online Privacy Rights Act, and Senator Roger Wicker’s Safe Data Act. The laws aim to bridge the gap and move privacy legislation forward. Legislators disagree on conceptual issues, enforcement, enforcement, Federalism, preemption, private rights of actions, on conceptual issues, enforcement, enforcement, Federalism, preemption, private rights of actions, and the First Amendment. [22]

- Conceptual Issues: Some proponents suggest applying a “prescriptive” approach in which the law defines data protection rules and obligations. The CCPA uses a prescriptive approach. Other proponents argue that an “outcome-based” model where legislation focuses on the outcomes of practices rather than defining the practices themselves. Another issue includes the types of data that the Federal government would regulate, whether it would include personal information or not. [23]

[21] “California Consumer Privacy Act (CCPA).” State of California - Department of Justice - Office of the Attorney General, July 14, 2021. https://oag.ca.gov/privacy/ccpa.
[22] Kerry, Cameron F., and John B. Morris. “Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation.” Brookings. Brookings, December 8, 2020. https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/.
[23] “Data Protection and Privacy Law: An Introduction - Congress.” Accessed October 1, 2021. https://crsreports.congress.gov/product/pdf/IF/IF11207

- Enforcement: The FTC is held accountable for enforcing data protection. However, the FTC can't punish first-time violation offenders, but it may authorize a cease and desist order. The FTC doesn't have jurisdiction over banks, nonprofits, or other carriers.
- Federalism and Preemption: Congress needs to structure the federal-state balance on federal programs and state policies. For a comprehensive system of data protection laws, Congress could preempt many state laws related to data protection. Congress could allow states to keep their laws intact or to render the laws invalid.
- First Amendment: There may be possible limitations due to the First Amendment under the Constitution. The Supreme Court has recognized that data protection laws implicate the first amendment, but the laws don't completely invalidate the laws. The nature of the regulatory law will determine its validity. For example, commercial purposes are subject to less scrutiny in court.
- Private Rights of Actions: Congress may establish a constituent's private right of action to sue a third party over a violation of the new data protection law. The injury may be difficult to prove. Victims of data breaches and privacy violations may have a hard time proving their case. Individuals must show concrete harm from a statutory violation.

Furthermore, the privacy rights of consumers have been impacted by the adoption of geolocation services. Geolocation data sharing has become a growing privacy issue with the government. The government has the authority to collect and use personal information like geolocation data. This practice has been increasingly controversial because some consumers see this as an invasive practice. Even though the data is anonymized, it is relatively easy to de-anonymize the data.

Before the pandemic, Congress and the FCC penalized invasive geolocation data-sharing among cell carriers. The FCC announced that it planned to impose a $200 million fine against major cell phone carriers Sprint and T-Mobile.[24]

[24] McAllister, K. (2020, April 29). *The biggest data privacy holes made worse by the pandemic*. Protocol. Retrieved November 20, 2021, from https://www.protocol.com/Braintrust/data-privacy-holes-coronavirus-pandemic?rebelltitem=6#rebelltitem6.

The merged company sold its user's real-time location data to third parties without consent from users. However, ever since the pandemic began, the cell carriers have re-branded to sell the same data to stop the coronavirus spread.

Under the pandemic lockdown, the mobile advertising industry was legally able to locate data from applications on consumers' phones and then hand that information to the federal or state government. [25] The federal government was able to acquire location data without needing to ask cellphone carriers directly for this set of information. Mobile advertising companies have begun to provide their data analyses of geolocation and movements to the Center for Disease Control and state and local governments. The federal government began its national coronavirus surveillance system to monitor and forecast rates of infection and hospitalizations in the United States.

Moreover, Senate Democrats have called on the Federal Trade Commission Chair Lisa Khan to write new rules to protect consumer data privacy in a letter to the agency in September 2021. Senator Richard Blumenthal and other Democrats sent a letter to "begin a rulemaking process" on privacy because "consumer privacy has become a consumer crisis.[26] The senators explained that technology companies have not kept their promises and have neglected their legal obligations. The senators felt that technology companies have received wrist-slap punishments while consumers have received minimal relief. President Joe Biden recently nominated privacy critic Alvaro Bedoya to become the third democratic FTC commissioner. The Senate has yet to schedule a confirmation hearing for him, but Bedoya has expressed interest in helping the FTC craft rulemakings in regards to privacy. The FTC rulemaking could help the government regulate the data privacy industry despite partisan differences.

In response to privacy concerns, United States Republican Senators Roger Wicker and Marsha Blackburn introduced Federal Data Privacy legislation in July 2021. The bill is titled S.499 "Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act.[27]

[25] *Mobile location data and covid-19: Q&A*. Human Rights Watch. (2020, October 28). Retrieved November 20, 2021, from https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.
[26] Kelly, M. (2021, September 20). *Senate Democrats call on FTC TO FIX data privacy 'crisis'*. The Verge. Retrieved November 20, 2021, from https://www.theverge.com/2021/9/20/22684394/ftc-data-privacy-facial-recognition-blumenthal-warren-khan.
[27] "Wicker, Blackburn Introduce Federal Data Privacy Legislation." U.S. Senate Committee on Commerce, Science, & Transportation, July 28, 2021. https://www.commerce.senate.gov/2021/7/wicker-blackburn-introduce-federal-data-privacy-legislation.

This law would give American consumers more choice and control over their data. The SAFE Data Act would also direct businesses to be more transparent and accountable about their data collection practices. This bill also increases the authority of the Federal Trade Commission's (FTC) authority and provides additional resources to enforce the legislation. The SAFE DATA Act would provide Americans with more control over their data by:

- Requiring businesses to allow consumers to access, correct, delete, and extract their data
- Preventing businesses from processing or transferring consumers' data without consent
- Prohibiting businesses from denying consumers products or services for their privacy rights
- Minimizing the amount of consumer data collected, processed, and retained by businesses and secondary uses of consumer data without consent
- Establishing data protection standards enforced by the Federal Trade Commission (FTC)

Policy Proposal: Data-Protection Legislation

The goal of this policy proposal is to establish the data privacy rights of 280 million American consumers at the federal level.[28] Data privacy is defined as the ability for a consumer to determine when, how, and to what extent personal information is shared with others.[29] The personal information may consist of an online user's electronic data, location information, and demographic information. The budgeted cost of this proposal is approximately 6.5 billion per year, as suggested by the Information Technology and Innovation Foundation.[30] This Data Protection law would be adopted through regulatory authorization and implementation in the following details.

Policy Authorization Tool:

Further, the data protection law would be authorized by Congress if passed. This legislative proposal was drafted by the United States, Senator Kirsten Gillibrand. Senator Gillibrand re-introduced bill S.2134 the Data Protection Act of 2021 (DPA) to protect Americans' data privacy through transparent and fair data practices. [31] The Data Protection Act includes authorization through supervision of Data Aggregators, office of civil rights, enforcement powers, penalties, and fines.

Moreover, the Privacy Act would grant an independent agency power to review Big Tech mergers. In this case, data aggregators are any person that collects, uses, or shares in or affecting interstate commerce, an amount of personal data that is not, de minimis, as well as entities related to that person by common ownership. The independent agency would review mergers consisting of large data aggregators, or a merger that impacts the transfer of personal data of at least 50,000 consumers. [31] Also, the Office of Civil Rights will help advance data justice and protect consumers from discrimination. Under the DPA, enforcement power to supervise the use of high-risk data practices to penalize, examine,

[28] Menezes, Andrew. "280 Million Americans Have No Control over Their Data. A National Standard Is the Only Way to Fix It." Roll Call. Roll Call, April 16, 2021. https://www.rollcall.com/2021/04/16/280-million-americans-have-no-control-over-their-data-a-national-standard-is-the-only-way-to-fix-it/.

[29] Cloudflare. (n.d.). *What is data privacy? | privacy definition | cloudflare*. What is data privacy? Retrieved November 21, 2021, from https://www.cloudflare.com/learning/privacy/what-is-data-privacy/.

[30] Castro, Daniel, and Alan McQuinn. "The Costs of an Unnecessarily Stringent Federal Data Privacy Law." The Costs of an Unnecessarily Stringent Federal Data Privacy Law. Information Technology and Innovation Foundation, August 5, 2019. https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.

[31] "Gillibrand Introduces New and Improved Consumer Watchdog Agency to Give Americans Control over Their Data: Kirsten Gillibrand: U.S. Senator for New York." Kirsten Gillibrand | U.S. Senator for New York, June 17, 2021. https://www.gillibrand.senate.gov/news/press/release/gillibrand-introduces-new-and-improved-consumer-watchdog-agency-to-give-americans-control-over-their-data.

or propose solutions to social, ethical, and economic impacts of data collection.

Further, high-risk data practice entails an action by a data aggregator that involves the use of an automated decision system, the processing of data in a way that includes a consumer's protected class, familial status, source of income, financial status, veteran status, criminal convictions, arrests, citizenship, past, present, or future physical or mental condition, and other facts used as a proxy to identify personal characteristics. High-risk practices can include the following: systemic processing of public data on a large scale, processing new technologies, combining new technologies that contribute to privacy harm, decisions about a consumer's access to a product, service, opportunity, or benefit which is based on an automated decision system processing, profiling of individuals at a mass scale, processing of biometric information to uniquely identify an individual, combine, comparing, or matching personal data, processing an individual's geolocation, processing personal data of minors under 17 or other vulnerable individuals such as the elderly, people with disabilities, and other groups known to susceptible for exploitation for marketing purposes, profiling, automated processing, or consumer scoring about the eligibility of an individual's rights, benefits, privileges, employment, credit, insurance, education, professional certification, and health services. High-risk data practice impact evaluations would be implemented to prevent data aggregators from committing unlawful, unfair, deceptive, abusive, discriminatory data practices about processing data, sharing data, and re-identifying an individual from anonymized data.[32] This Act would focus on giving Americans more control and protection over their data by authorizing and enforcing data protection rules. Online users would have the ability to file complaints, receive injunctive relief, and equitable damages.

[32] Gillibrand, K. (2021, June 12). *S.2134 - Data Protection Act of 2021*. Congress.Gov. Retrieved from https://www.congress.gov/bill/117th-congress/senate-bill/2134/text?q=%7B%22search%22%3A%5B%22data+protection+2021%22%2C%22data%22%2C%22protection%22%2C%222021%22%5D%7D&r=1&s=1.

Policy Implementation Tool:

Under this Act, the Data Protection Agency would have a director appointed by the President and confirmed by the Senate to serve a 5-year term.[33] The Director would prescribe rules, issue orders, and guidance to administer and carry out the objectives of this Act. This agency would investigate, subpoena for testimonies and documents, and issue civil investigative demands. The agency could issue regulations after notice and under section 533 of the United States Code. The Agency could prescribe rules to data aggregators or service providers upon identifying high-risk practices in connection to the collection, processing, and sharing of personal data which may include requirements for auditing, preventing, or restricting such acts. The agency can prescribe rules for acts or practices about collecting, processing, and sharing personal data that cause privacy harm to individuals. The agency could also prescribe rules for unfair, deceptive, abusive, or discriminatory acts or practices with the collection, processing, or sharing of personal information. The agency would ensure that data aggregators provided individuals with the right to access and correct, or limit the processing of, and request deletion of personal data. Rules could also be prescribed to obligate data aggregators for transparency, data collection limits and disclosure limitations, processing requirements, accountability requirements, confidentiality requirements, security requirements, and data accuracy requirements.[33]

Further, this proposal includes policies that discourage businesses from violating the rules. This Agency would use tools that include civil penalties, injunctive relief, and equitable remedies to punish offenders of the data privacy rules. The Agency would manage complaints, investigations, and information for the public on data protection issues. For example, the Data Protection Agency could launch an investigation regarding a data aggregating business, share its findings, issue penalties, and civil action, as well as relief business. [34] The DPA Director could impose a charge on the data aggregator

[33] Gillibrand, K. (2021, June 12). *S.2134 - Data Protection Act of 2021*. Congress.Gov. Retrieved from https://www.congress.gov/bill/117th-congress/senate-bill/2134/text?q=%7B%22search%22%3A%5B%22data+protection+2021%22%2C%22data%22%2C%22protection%22%2C%222021%22%5D%7D&r=1&s=1.

[34] Gillibrand, Kirsten. "Sil 21697." SIL21697 N61. United States Senate. Accessed October 12, 2021. https://www.gillibrand.senate.gov/imo/media/doc/2021%20DPA%20(Gillibrand)%20-%20Section%20by%20Section.pdf.

that has annual gross revenue over $25,000,000 and the personal data of 50,000 individuals, households, or devices. The Director would impose appropriate penalties. [35] Penalties can be tripled for violations against minors under this law. High-risk data practice assessments would be conducted to determine the high-risk practice and high-risk data development process, including the design and training of the high-risk data practice for the likelihood of accuracy bias, discrimination, privacy harms in system designs, methodologies, and training data characteristics. An assessment of the benefits and costs of high-risk data practices would be conducted to determine the unintended consequences when taking into consideration the data minimization practices, the duration and methods of personal data and results of storing high-risk data, the available information, the extent to which individuals have access to the results of the high-risk data practice, and may correct the results, and the recipients of the results of the high-risk practices.

Then, the Agency would maintain that the technology sector remained fairly competitive in the digital marketplace. Under this proposal, the agency's research unit would analyze and report on data protection and privacy innovation to both the private and public sectors. This agency would develop and provide resources that assess unfair, deceptive, and discriminatory outcomes that result from algorithms. Also, the agency would develop privacy and data protection guidelines and policies for the private sector. Compliance with the rules would help small businesses to be better prepared for cyberattacks. In practice, the Agency would coordinate with federal and state regulators to promote consistent regulatory standards of personal data.

Additionally, while this proposal does not include policies that encourage compliance, I would like to add a section to grant small and medium businesses a tax incentive for compliance with the Privacy Act rules after one year. Businesses would have to prove that their compliance with the Act. The Data Privacy Agency would be tasked with determining the monetary details of this incentive.

Next, a media campaign would help to increase awareness of the implementation of the Privacy

[35] The Regulatory Review. "A New Digital Age Privacy Protection Agency Holds Promise." The Regulatory Review, August 8, 2021. https://www.theregreview.org/2021/08/09/allen-new-digital-age-privacy-protection-agency-holds-promise/.

Act among businesses and consumers. Federal and state agencies would help to promote this campaign to American consumers. The media campaign would be run for three months once the Act has passed through Congress. Over 250 million consumers will be targeted through this campaign which includes online ads and partnerships with state agencies for public announcements. The Privacy Act would take effect starting in November 2022.

Lastly, the budgetary cost of this legislative proposal is estimated to be 6.5 billion. The cost is associated with compliance costs. The costs associated with hiring privacy personnel will cost small, medium, and large businesses are approximately 6.3 million. Over 60,000 data protection officers would be necessary to hire for compliance purposes for all businesses.[36] Privacy audits for all American organizations that handle personal data would cost $440 million, according to the Information Technology, and Innovation Foundation.[36] Though these figures take into account all American businesses, the legislation will only target businesses that handle personal data. Overall, the federal government would need to consider the associated costs that are incurred on businesses under this proposal. It is important to note that by not including deletion, data portability, and rectification, this legislation is not incurring around $7.2 billion in costs associated with these activities.

Policy Analysis

The Data Protection Act of 2021 proposed guidelines for businesses to protect personal data. Senator Kirsten Gillibrand proposed this S.2134 bill to ensure that companies would not mine data from personal purchases, conversations via smart devices, and the privacy rights of individuals. While this is the most recent data privacy protection proposal, it has advantages and disadvantages. It is primarily important to consider the effectiveness and viability of this Act.

[36] Castro, Daniel, and Alan McQuinn. "The Costs of an Unnecessarily Stringent Federal Data Privacy Law." The Costs of an Unnecessarily Stringent Federal Data Privacy Law. Information Technology and Innovation Foundation, August 5, 2019. https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law

Effectiveness: Will Policy Achieve the Stated Goal?

The goal of this policy proposal is to establish the data privacy rights of American consumers at the federal level. A key component of this bill is the creation of a Data Protection Agency which would have broad rulemaking authority and resources to effectively enforce data protection rules created by itself or Congress. The Data Protection Agency would have the enforcement tools such as civil penalties, injunctive relief, and equitable remedies. Additionally, the Data Protection Agency's research unit would analyze and report on data protection and privacy.[37] The research unit's goal is to focus on assessing unfair outcomes that result from the use of automated decision systems such as algorithms. Under the Data Protection Act, the bill would join 80 other countries in the enforcement of data privacy protection. For example, Canada passed its Consumer Privacy Protection Act (CCPA). The CCPA grants portability of data rights to consumers expands requirements for consent and imposes fines up to 5% of global revenue or $25 million against companies for serious offenses of privacy legislation. Consumers in Canada have access to their data and protection of their data compared to consumers in America.[38] The S.2134 bill would establish an authorizing entity to oversee data aggregating companies. The bill would effectively attempt to establish the data privacy rights of consumers.

Disadvantages of Proposal

The Data Protection Act 2021 has its disadvantages to consider in terms of legality. One disadvantage is that the Act would differ from some state data privacy laws that are currently in effect in Virginia, California, Colorado. These three states have enacted their own comprehensive consumer data privacy laws which have provisions that include the right to access and delete personal information and opt-out of the sale of personal information, according to the National Conference of State Legislatures. Ultimately, the state laws could be overridden by the federal privacy protection legislation. [39]

[37] Gillibrand, Sen. Kirsten. "Americans Need a Data Protection Agency." Medium. Medium, June 17, 2021. https://gillibrandny.medium.com/americans-need-a-data-protection-agency-f19ff786bfca.

[38] DLA Piper. (2021, January 28). *Data Protection Laws of the World*. Law in Canada - DLA Piper Global Data Protection Laws of the World. Retrieved November 19, 2021, from https://www.dlapiperdataprotection.com/index.html?t=law&c=CA.

[39] Greenberg, Pam. State laws related to Digital Privacy. National Conference of State Legislatures. Accessed November 1, 2021. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

Another disadvantage of this proposal is the high costs of the necessary administrative capacity. Under this proposal, the administrative capacity is high due to the creation of a new agency. The Data Protection Agency would be similar to the Consumer Financial Protection Bureau because it enforces data protection rules created by either the agency or Congress to ensure that data practices are fair and transparent. It is important to consider the administrative costs of having a similar agency because the fiscal year budget totals over $500 million per year, according to the Consumer Financial Protection Bureau. [40] The Consumer Financial Protection Bureau is funded through the earnings of the Fed. The Data Protection Act's budget would be similar to the Consumer Financial Protection Bureau's budget.

Further, the Act may be efficient at granting consumers more control over their online activities without targeted advertising. Consumers may not be able to recognize the direct impact immediately, but it could lead to less targeted advertising and more irrelevant advertising. This may negatively affect consumers who benefit from targeted advertisements. According to Wharton Professor Eric Bradlow, "advances in targeted advertising in the past 15 or 20 years, and one is that we do better targeting because we have better data. The other is machine learning and our ability to find patterns we couldn't find before, and computing and cloud computing will allow us to do more in a faster time." [41] Ultimately, consumers could explore online activities freely with less targeted advertising than they have now.

Advantages of Proposal:

The Data Protection Act has the advantage of providing fairness to consumers. According to the proposal, the agency's research unit would focus on analyzing and reporting on data protection and privacy innovation in the private and public sectors. If the research unit were successful, then it would measure the relative costs and benefits of high-risk practices that create spillover effects and disparate impact and privacy harms on consumers. The research team would measure the relative costs and benefits that affect consumers. This team has the potential to change the discriminative impact in their ex-ante risk assessment and the ex-post impact evaluation of high-risk data which could benefit consumers.

[40] "Fiscal Year 2020: Annual Performance Plan and Report, and ..." Fiscal Year 2020: Annual performance plan and report, and budget overview. Bureau of Consumer Financial Protection, February 2020. https://files.consumerfinance.gov/f/documents/cfpb_performance-plan-and-report_fy20.pdf.
[41] University of Pennsylvania. "How Will Targeted Ads Fare in an Era of Data Protection?" Knowledge@Wharton. University of Pennsylvania, June 22, 2018. https://knowledge.wharton.upenn.edu/article/will-targeted-ads-fare-era-data-protection/.

The Data Protection Act would provide uniformity of rules for businesses to follow. Currently, state laws are setting specific guidelines for data aggregators. Companies have different state laws to abide by in California versus in Virginia. However, under one federal law, businesses would have one uniform set of guidelines instead of differing state guidelines.

Viability: Likely Contentions

As Americans have become more active on online applications, privacy legislation has become increasingly popular at the federal level. Data privacy laws will likely be passed at the Congressional level in the future. However, there are some differences in legislative proposals. Key points of the debate have included whether and to what extent the law should preempt more stringent state laws. Another point of debate is whether legislation should include a private right of action. Despite these differences, states like California have passed their privacy protection laws which may be difficult for federal legislation to preempt those state laws entirely because the federal framework would need to be more stringent, according to Gibson Dunn.[42]

Additionally, under the new Biden administration, he intends to renew the Consumer Privacy Bill of Rights that was proposed by President Barack Obama. The bill seeks to add strong national standards protecting consumers' privacy rights. President Biden is also interested in updating the Electronic Communications Privacy Act to increase the protection of digital content to be treated as physical content.

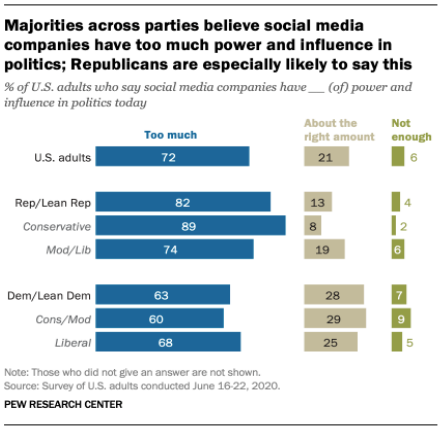
Furthermore, policymakers on both parties are concerned about Section 230 of the Communications Decency Act which includes the scope of immunity that courts have accorded to social media companies under this law.[42] The Department of Justice has proposed updating this law to include limitations on immunity. Republicans are concerned with the anti-conservative bias on social media that is self-regulated. Democrats are concerned about the spread of misinformation and hate speech that is promoted on social media. While the Data Privacy Act research team aims to research these topics, regulating changes may prove to be challenging.

[42] "U.S. Cybersecurity and Data Privacy Outlook and Review – 2021." Gibson Dunn, June 22, 2021. https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2021/.

Political Analysis:

Passage of the Data Privacy Act would likely increase your chance of re-election in the 2022 midterms cycle. The public supports government regulation of technology companies. The Pew Research Center conducted a poll in June 2020 and found that half of Americans say major tech companies should be regulated by the government more than they are now. The polling data found that 72% of adults said that social media companies have too much power and influence in politics. The graph below indicates this view. [43] The passage of this bill could increase the public trust that consumers have in the federal government since they believe that technology companies have too much power and influence in politics.

Figure 2. Pew Research Survey on Social Media Companies



Moreover, since your congressional district, VA-10 is a swing district, it's important to pass legislation that could help your likelihood of being elected. Importantly, a recent Suffolk University poll released this week indicated that Republicans are leading Democrats in the congressional ballot by 8 points in Virginia. House Democrats are vulnerable in the 2022 midterms cycle, according to Hill.[44] It would be strategic to pass legislation that is popular among both Republicans and Democrats in VA-10.

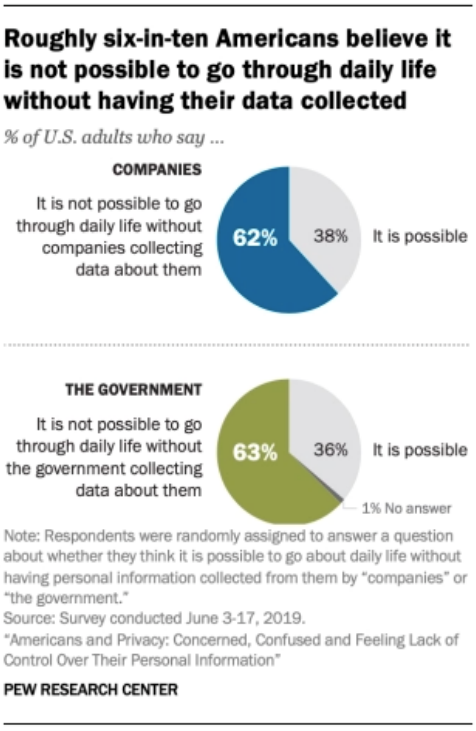
Also, in 2019, the Pew Research Center surveyed data collection and found that 60% of Americans said they do not think it is possible to go through daily life without having their data collected

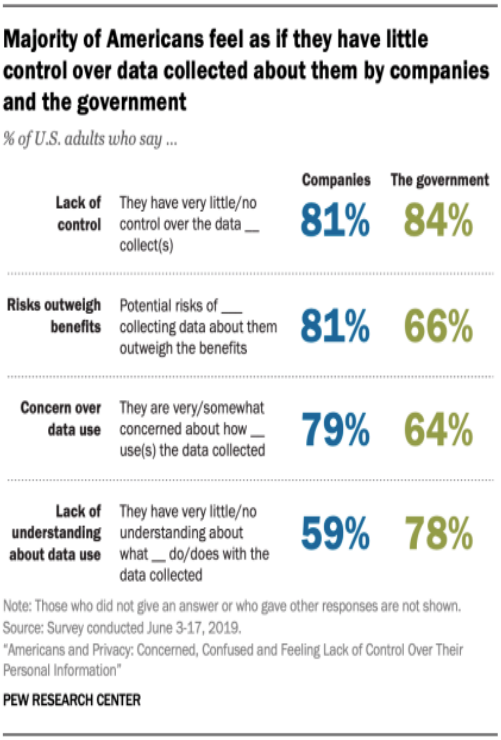
[43] Auxier, B. (2020, October 27). *How Americans see U.S. tech companies as government scrutiny increases*. Pew Research Center. https://www.pewresearch.org/fact-tank/2020/10/27/how-americans-see-u-s-tech-companies-as-government-scrutiny-increases/.

[44] Manchester, J. (2021, November 11). *Virginia emerging as Ground Zero in battle for House majority*. TheHill. Retrieved November 10, 2021, from https://thehill.com/homenews/campaign/581050-virginia-emerging-as-pivotal-in-battle-for-house-majority.

by companies or the government.[45] The graph below shows that most Americans believe that data is collected daily. The polling data also indicated that 80% of Americans are concerned about the collection of their data. [45] These issues are addressed in the Data Protection Act. The passage of the Data Protection Act bill would help to address the privacy concerns of your constituents.

Figure 3 & 4: Pew Research Survey on Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Personal Information





Further key stakeholders in the privacy protection legislation debate include members of Congress, the Federal Trade Commission, constituents, think tanks, and companies that collect consumer data. Democrat and Republican Congressional members have proposed their federal data privacy protection laws. Over the past years, dozens of privacy regulation bills have been proposed in Congress. Republican and Democratic legislators have addressed individual rights, business obligations, and special protections for sensitive information, and access to records by law enforcement in their proposals.

[45] Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, August 17). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center: Internet, Science & Tech. Retrieved November 10, 2021, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Below, you can see a list of data privacy bills proposed this year by both chambers.[46]

Figures 5-8: Bills in Chamber (117th Congress)

Bills In Both Chambers (117th Congress)

	House number	Senate number	Title	Key provisions	State law pre-emption	Private right of action	Sponsor
BILLS IN BOTH CHAMBERS	H.R.651	S.81	Public Health Emergency Privacy Act	• Restricts use and disclosure of COVID-19 emergency health data.	⊗	✓	Rep. Eshoo, Anna; Sen. Blumenthal, Richard
	H.R.778	S.199	Secure Data and Privacy for Contact Tracing Act of 2021	• Creates grants to develop technology for contact tracing in COVID-19 that meet privacy, security and other standards.	N/A	N/A	Rep. Speier, Jackie; Sen. Schatz, Brian
	H.R.847	S.224	Promoting Digital Privacy Technologies Act	• Directs the National Science Foundation to support research grants for privacy-enhancing technologies.	N/A	N/A	Rep. Stevens, Haley; Sen. Cortez Masto, Catherine
	H.R.2039	S.1209	Protecting Investors' Personally Identifiable Information Act	• Prohibits the Securities and Exchange Commission from requiring personally identifiable information be collected for audit trail reporting requirements.	N/A	N/A	Rep. Loudermilk, Barry; Sen. Kennedy, John
	H.R.2738	S.1265	Fourth Amendment Is Not For Sale Act	• Prevents law enforcement and intelligence agencies from "obtaining subscriber or customer records in exchange for anything of value."	N/A	N/A	Rep. Nadler, Jerrold; Sen. Wyden, Ron
	H.R.3868	S.1932	No Vaccine Passports for Americans Act (House); No Vaccine Passports Act (Senate)	• Prohibits establishment of a federal vaccine passport and provides for nondiscrimination in employment, in public accommodation, by public entities and in access to federal services based on vaccination status.	⊗	⊗	Rep. Harshbarger, Diana; Sen. Cruz, Ted

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS • IAPP.ORG • FEDERAL PRIVACY BILLS - 117TH CONGRESS • BILLS IN BOTH CHAMBERS

	Number	Title	Key provisions	State law pre-emption	Private right of action	Sponsor
SENATE BILLS	S.1494	Consumer Data Privacy and Security Act of 2021	• Provides consumers with rights to access, correct and delete their data. • Requires businesses to implement data security programs. • Prohibits collection without consumers' consent.	✓	⊗	Sen. Moran, Jerry
	S.1628	Children and Teens' Online Privacy Protection Act	• Extends privacy protections to children aged 12-16, including the provision of notice and consent.	⊗	⊗	Sen. Markey, Edward
	S.1667	Social Media Privacy Protection and Consumer Rights Act of 2021	• Grants users of online platforms the right to opt out of data collection and tracking, provides users with the right to access, requires "plain English" terms of service agreements, and mandates establishment of privacy and security programs.	⊗	⊗	Sen. Klobuchar, Amy
	S.2052	Facial Recognition and Biometric Technology Moratorium Act of 2021	• Prohibits biometric surveillance by the federal government without explicit statutory authorization.	⊗	✓	Sen. Markey, Edward
	S.2134	Data Protection Act of 2021	• Establishes an independent federal "Data Protection Agency" to regulate high-risk processing and use of personal data.	N/A	N/A	Sen. Gillibrand, Kirsten
	S.2499	Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act	• Requires companies to publish privacy policies, appoint privacy and data protection officers, implement customers' rights to correction and deletion, and minimize the data they collect.	✓	⊗	Sen. Wicker, Roger

[46] Fazlioglu, M. 2021. US Federal Privacy Legislation Tracker. Retrieved November 10, 2021, from https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/.

	Number	Title	Key provisions	State law pre-emption	Private right of action	Sponsor
SENATE BILLS	S.24	Protecting Personal Health Data Act	• Directs Department of Health and Human Services to regulate consumer devices, services, apps and software that collect or use personal health data.	N/A	N/A	Sen. Klobuchar, Amy
	S.47	APP Act	• Requires operators from specified countries that make their software available to U.S. consumers to disclose to the Federal Trade Commission and Department of Justice certain information, including any data protection measures in place. • Prohibits data collection from U.S. users if the operator complies with requests from specified foreign governments to disclose U.S. consumer data.	✓	✗	Sen. Rubio, Marco
	S.113	BROWSER Act of 2021	• Requires covered entities to obtain users' opt-in approval to use their sensitive information and opt-out approval to use their non-sensitive information.	✓	✗	Sen. Blackburn, Marsha
	S.500	Stop Marketing And Revealing The Wearables And Trackers Consumer Health Data Act	• Prohibits the transfer or sale of consumer health information collected from a "personal consumer device" to entities whose primary business function is to collect or analyze consumer information for profit, unless it obtains the consumer's informed consent.	✗	✗	Sen. Cassidy, Bill
	S.919	Data Care Act of 2021	• Imposes various responsibilities on online service providers with respect to their handling of identifying data, including securing it from unauthorized access and preventing harm.	✗	✗	Sen. Schatz, Brian
	S.1444	Mind Your Own Business Act of 2021	• Requires assessments, periodic reporting and opt-out processes by covered entities that operate high-risk or automated decision-making information systems, such as AI or machine learning. • Imposes criminal penalties for false certification of annual reports by corporate officers.	✗	✓	Sen. Wyden, Ron

	Number	Title	Key provisions	State law pre-emption	Private right of action	Sponsor
HOUSE OF REPRESENTATIVES BILLS	H.R.474	Protecting Consumer Information Act of 2021	• Requires the FTC to review and potentially revise its current privacy standards with respect to whether they are sufficient to protect consumers' financial information from cybersecurity threats.	N/A	N/A	Rep. Lieu, Ted
	H.R.1781	PROTECT Kids Act	• Amends the Children's Online Privacy Protection Act of 1998 by expanding its scope to include services provided through mobile applications, precise geolocation and biometric information, and to children up to the age of 16.	N/A	N/A	Rep. Walberg, Tim
	H.R.1816	Information Transparency & Personal Data Control Act	• Requires use of "plain English" privacy policies, opt-in for sensitive information, imposes transparency requirements and mandates biannual privacy audits.	✓	✗	Rep. DelBene, Suzan
	H.R.1871	Transportation Security Transparency Improvement Act	• Addresses policies of the Transportation Security Administration related to Sensitive Security Information, affecting air carriers, airport operators, and state and local law enforcement.	N/A	N/A	Rep. Bishop, Dan
	H.R.2384	No Vaccine Passports Act	• Prohibits federal agencies from issuing vaccine passports or passes to certify COVID-19 vaccination status or publishing or sharing COVID-19 records or any similar health information of U.S. citizens.	N/A	N/A	Rep. Biggs, Andy
	H.R.2980	Cybersecurity Vulnerability Remediation Act	• Amends the Homeland Security Act of 2002 and establishes an incentive-based program to encourage industry, academia and individuals to provide "remediation solutions for cybersecurity vulnerabilities."	N/A	N/A	Rep. Jackson Lee, Sheila

Moreover, as technology advances, data collection will continue to impact the daily lives of individuals. Privacy protection legislation will inevitably be passed by Congress in the future. The number of proposals suggests that privacy protection is important. It will benefit your political reputation to vote in favor of data protection laws. Various stakeholders have publicly announced their support for privacy and cybersecurity legislation.

[46] Fazlioglu, M. 2021. US Federal Privacy Legislation Tracker. Retrieved November 10, 2021, from https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/.

Furthermore, the United States Chamber of Commerce assembled a list of key stakeholders in data privacy protection. A key privacy advocate who helped to draft the California Consumer Privacy Act (CCPA), Alastair Mactaggart, explained that the CCPA would set the framework for any federal privacy legislation. He indicated that Congressional legislators from California, which make up 20% of the House Democratic Caucus would not approve of any law that undermined the consumer rights established under the California Consumer Privacy Act.[47]

As indicated earlier, the Federal Trade Commission is a key stakeholder, because they have penalized technology companies for deceptive practices with the personal data of consumers. Federal Trade Commissioner Noah Phillips indicated that does not speak for the Commission, but he does support comprehensive federal privacy legislation. He suggested that the Federal Trade Commission is an appropriate authority for the enforcement of privacy regulations.

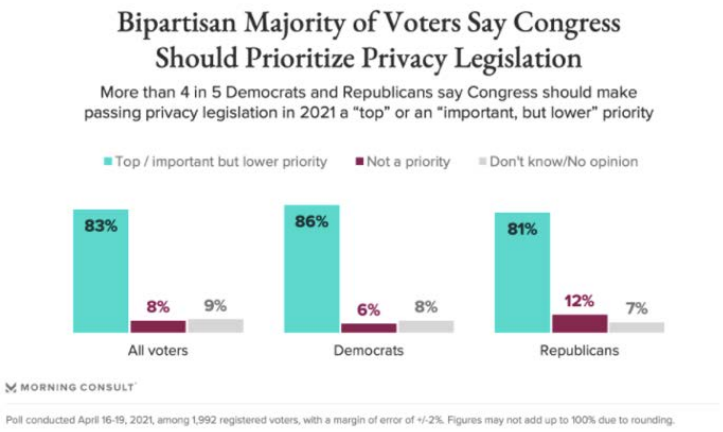
Stakeholders like Cathy McMorris Rodgers (R-WA) advocate for federal legislation that avoids the negative effects on small businesses and innovation. Congresswoman Rodgers is an opponent of legislation that includes a private right of action. She believes that lawsuits would benefit attorneys instead of consumers. Proponents like Congresswoman McMorris believe that the benefits of businesses using data provide consumers with time-efficient, higher quality customer service, and targeted loyalty programs. The impact on business plays a key role for some privacy legislation proponents like Rodgers.

Stakeholders such as Senator Roger Wicker (R-MS) AND Marsha Blackburn (R-TN) re-introduced the SAFE DATA Act in the Senate this year. Unlike the Data Protection Act, the SAFE DATA Act establishes a comprehensive privacy framework that includes consent requirements for sensitive data, data subject rights, and privacy policy requirements. This SAFE DATA Act would preempt state laws, while the Data Protection Act of 2021 would not preempt state laws. As a result, the SAFE DATA Act and the Data Protection Act of 2021 have not proceeded beyond committee assignments.

[47] *U.S. Chamber of Commerce assembles key stakeholders to discuss data privacy*. Technology Law Dispatch. (2019, October 16). Retrieved November 10, 2021, from https://www.technologylawdispatch.com/2019/07/regulatory/u-s-chamber-of-commerce-assembles-key-stakeholders-to-discuss-data-privacy/.

Stakeholders such as voters indicated in a Morning Consult Poll that 4 in 5 Democrats and Republicans say Congress should make privacy legislation a “top” or an "important, but lower" priority. Over 20 states have introduced their data privacy bills in 2021 to address the concerns of Americans. [48] Technology companies are anticipated to push Congress to act, so they don’t have to figure out the compliance with a patchwork of state laws.

Figure 9. Morning Consult Poll on Privacy Legislation



While this proposal would provide constituents with federal privacy protections, one clear disadvantage is the controversy among privacy advocates. The Data Protection Act of 2021 would not allow for the pre-emption of state laws that have been passed. Advocates of the California Consumer Protection Act such as Alastair Mactaggart would not be satisfied. The Data Protection Act does not include the right of private action to sue companies that mishandle personal data.[49] This is a civil right that would be taken away from consumers in California. Supporters of the CCPA have considered this to be a similar framework to the EU's GDPR. Elimination of these consumer rights would send a message of distinction from the EU's stance on privacy rights. In terms of advantages, the Data Protection Act would oblige companies to follow a uniform set of rules rather than a patchwork of varying state laws. The Data

[48] *States are moving on privacy bills. Over 4 in 5 voters want Congress to prioritize the protection of online data*. Morning Consult. (2021, April 28). Retrieved November 15, 2021, from https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/?mkt_tok=ODUwLVRBQS01MTEAAAF8tGdTLpPMEkRnSBZ1p0er2xMS3KaYhx47zjkh_KVgJwTwBI7dvufmlcpFnDJOFSs6qpN2LhnRZHB8W181YDd3zcWVtpeZ8GCepzXgcDvAeuI.

[49] *More privacy, please - September 2021*. Troutman Pepper - More Privacy, Please - September 2021. Retrieved November 10, 2021, from https://www.troutman.com/insights/more-privacy-please-september-2021.html.

Protection Act could gain support from Republican lawmakers who do not support the private right of action to sue companies or stunt business innovation. Due to the bipartisan nature of this bill, the passage of it would benefit the interests of your constituency.

Policy Recommendation:

My recommendation is that you proceed in supporting of S.2134 bill. Opponents of the Data Protection Act like Cathy McMorris Rodgers (R-WA) believe that it will have negative effects on small businesses and innovation. Opponents don't support a consumer's right to sue technology companies based on privacy harm. However, the advantages of the Data Protection Act of 2021 outweigh its disadvantages.

Voting in support of the Data Protection Act would help to aid the data privacy concerns of voters ahead of the 2022 midterms cycle. The Data Protection Act would investigate any consumer complaints regarding deceptive practices. Also, the Data Protection Agency would have a rule-making authority over data aggregators. The Data Protection agency would help to keep data aggregators accountable to rules with its investigation and research capacity.

Also, voting in support of the Data Protection Act could position you to be re-elected as well. Since re-election is next year, the window of opportunity to pass legislation is closing. It would benefit you and your constituents to vote in support of S.2134 to further protect the privacy rights of consumers. Polling data from the Morning Consult indicated that privacy legislation is a top concern for over 80% of voters.[50] By voting in support of the S.2134 bill, it would signal to your constituents that you are prioritizing their concerns.

[50] *States are moving on privacy bills. Over 4 in 5 voters want Congress to prioritize the protection of online data*. Morning Consult. (2021, April 28). Retrieved November 15, 2021, from https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/?mkt_tok=ODUwLVRBQS01MTEAAAF8tGdTLpPMEkRnSBZ1p0er2xMS3KaYhx47zjkh_KVgJwTwBI7dvufmlcpFnDJOFSs6qpN2LhnRZHB8W181YDd3zcWVtpeZ8GCepzXgcDvAeuI.

Curriculum Vitae

Cristy Villalobos Hauser, is a native from North Carolina. She attended Meredith College in Raleigh as an undergraduate student. Cristy received her Bachelor of Arts in Political Science. She is a member of the political science honors society. Cristy worked as a legislative intern under House Representative Beverly Earle at the North Carolina General Assembly for three legislative sessions. Then, she conducted advocacy work for WomenNC in North Carolina and at the United Nations.

Upon graduation, Cristy moved to Virginia in 2017 to help elect over Democrats. She worked as an organizer, campaign director, and consultant for nonprofits and candidates in Northern Virginia. She hopes to graduate with a Master of Arts in Public Management in December 2021.